***Korporátní pravidla IMS a bezpečnosti a ochrany dat***

* 1. *Dodavatel je povinen při poskytování plnění dle Smlouvy/Objednávky dodržovat požadavky následujících mezinárodních standardů jak vyplývá z následující tabulky:*

|  |
| --- |
| *Systém* |
| *Systém managementu kvality podľa ISO 9001* |
| *Systém environmentálneho managementu podľa ISO 14001* |
| *Systém managementu bezpečnosti informácií podľa ISO 27001* |
| *Systém riadenia kontinuity podľa ISO 22301* |
| *Systém manažmentu služieb v informačných technológiách podľa ISO 20000-1* |

* 1. *Dodavatel je povinen poskytovat plnění a zabezpečit výkon činností, ke kterým se zavázal podle Smlouvy/Objednávky, primárně prostřednictvím svých kmenových zaměstnanců. Dodavatel není oprávněn pověřit výkonem svých povinností podle Smlouvy/Objednávky žádného subdodavatele bez předchozího souhlasu společnosti Slovak Telekom, a.s. (dále ST) / T-Mobile Czech Republic a.s. (dále TMCZ). Dodavatel může o takový souhlas požádat zasláním žádosti na email: security@t-mobile.cz, kde přiloží vyplněný dokument, který je uveden v příloze č.3 dokumentu Korporátní pravidla IMS a bezpečnosti a ochrany dat.*

* 1. *Pokud ST/TMCZ udělí Dodavateli souhlas s použitím konkrétního subdodavatele, je Dodavatel povinen uzavřít se subdodavatelem smlouvu, která zabezpečí, aby subdodavatel vykonával povinnosti podle této Smlouvy/Objednávky za stejných podmínek a ve stejné kvalitě, jako je dohodnuto mezi ST/TMCZ a Dodavatelem v  Smlouvě tak, aby bylo zajištěno dodržení požadavků ST/TMCZ stanovených Smlouvou. Dodavatel je plně odpovědný za řádné a včasné plnění těchto povinností subdodavatelem. Zejména, ale ne výlučně, se subdodavatel musí zavázat k dodržování ust. dokumentu Korporátní pravidla IMS a bezpečnosti a ochrany dat včetně jejích příloh, na které se tento článek odvolává. Zejména musí být se subdodavatelem písemně ujednány podmínky pro přístup, práva a povinnosti týkající se zabezpečení ochrany Důvěrných informací.*
  2. *V případě, že má Dodavatel certifikovaný nebo zavedený systém, jak je pospáno v bodě1. výše, pak je povinen předložit ST/TMCZ k nahlédnutí a kontrole dokumentované informace (např.: dokumenty, záznamy, logy, nahrávky) související s požadavky výše popsaných systémů, a to za účelem prokázání souladu s těmito systémy, jakož i se Smlouvou. V případě, že Dodavatel poskytuje plnění dle Smlouvy/Objednávky za pomoci a/nebo prostřednictvím svchálených subdodavatelů, kteří mají některý ze systémů certifikovaný či zavedený, zajistí Dodavatel souhlas s provedením auditů i u těchto subdodavatelů a to za účelem prověření shody s předmětnými normami.*
  3. *V případě, že Dodavatel nemá některý systém certifikovaný ani zavedený, souhlasí s provedením auditů zaměřených na prověření shody s požadavky Smlouvy/Objednávky. Dodavatel je povinen poskytnout zaměstnancům ST/TMCZ nebo jimi pověřeným osobám při výkonu auditu nebo při analýze rizik součinnost, předložit k nahlédnutí a ke kontrole dokumentované informace (např.: dokumenty, záznamy, logy, nahrávky), umožnit přístup do prostor a systémů souvisejících s plením podle Smlouvy/Objednávky. V případě, že Dodavatel poskytuje plnění dle Smlouvy/Objednávky za pomoci a/nebo prostřednictvím schválených subdodavatelů, kteří nemají některý ze systémů zavedený či certifikovaný, zajistí Dodavatel souhlas s provedením auditu i u těchto subdodavatelů a to za učelem prověření shody se Smlouvou.*
  4. *Dodavatel a jeho subdodavatelé jsou povinni v dohodnutých termínech vykonat činnosti a/nebo zavést nápravná opatření, která byla nalezena a dohodnuta jakožto výstup z auditu Dodavatele. Stejně tak jsou povinni vykonat činnosti a zavést nápravná opatření nalezená např. při testech, cvičeních, incidentech, řízení rizik. Dodavatel poskytne ST/TMCZ veškeré informace (např. zprávy z auditů), které se týkají schopnosti Dodavatele poskytovat plnění dle Smlouvy/Objednávky ST/TMCZ. Pokud zavedení nápravných opatření bude trvat déle, jak 30 dní a nebude-li v konkrétním případě dohodnuta jiná lhůta a/nebo plán pro zajištění nápravy nebude ST/TMCZ schválen nebo takový plán nezajistí nápravu, bude takový stav automaticky považován za podstatné porušení Smlouvy/Objednávky.*

* 1. *Dodavatel musí mít zavedený systém řízení kontinuty činností, aby byl schopen ST/TMCZ poskytovat plnění dle Smlouvy/Objednávky v případě nestandardních a neočekávaných situacích nepřetržitě a v souladu s parametry a kvalitou dohodnutou mezi smluvními stranami. Dodavatel je povinen poskytnout TMCZ/ST součinnost při přípravě a provádění plánů kontinuity činností nebo obnovy po havárii u ST/TMCZ. Dodavatel je povinen při poskytování plnění dle Smlouvy/Objednávky dodržovat požadavky na řízení kontinuity činností uvedené v příloze č. 2 dokumentu Korporátní pravidla IMS a bezpečnosti a ochrany dat za predpokladu že plnění bude vyhodnocené z BIA jako kritické a/nebo existuje zákonný důvod pro řízení Dodavatele v oblasti BCM.*
  2. *Dodavatel je povinný nakládat s odpady, kterých je původce či vlastníkem, v souvislosti s plněním dle Smlouvy/Objednávky, v souladu s obecně závaznými právními předpisys upravujícími oblast odpadů.*
  3. *Pověřené osoby Dodavatele vstupující do prostor a objektů ST/TMCZ a vykonávající tam činnost dle Smlouvy/Objednávky, jsou povinny seznámit se s dokumentací BOZP, požární ochranou a požárně-technickými zařízeními umístěných v prostorách objektu.*
  4. *Smluvní strany berou na vědomí a souhlasí s tím, že veškeré informace obsažené ve Smlouvě /Objednávce a informace vyměněné mezi smluvními stranami v souvislosti s poskytováním plnění dle Smlouvy/Objednávky, budou považovány za důvěrné a chráněné v rozsahu podmínek dohodnutých ve smlouvě o zachování důvěrnosti informací uzavřené mezi smluvními stranami (dále jen jako „NDA“).*
  5. *Není-li v této Smlouvě uvedeno jinak, jsou smluvní strany povinny vytvořit, používat a udžovat přiměřené technické, organizační a personální bezpečnostní opatření k zajitění důvěrnosti, dostupnosti a integrity Důvěrných informací. Tato opatření musí být dostatečně odolná proti náhodnému a/nebo neoprávněnému zničení, ztrátě, záměně, zpřístupnění a/nebo proti jakýmkoliv formám neoprávněného užívání Důvěrných informací. Smluvní strany jsou povinny udržovat tato opatření funkční po celou dobu užívání Důvěrných informací.*
  6. *Při poskytování  plnění dle Smlouvy/Objednávky je Dodavatel odpovědný za to, že plnění bude dodáno bez vad, s náležitou péčí a v souladu s přílohou č. 1 dokumentu Korporátní pravidla IMS a bezpečnosti a ochrany dat.*
  7. *Dodavatel prohlašuje, že plnění dle Smlouvy/Objednávky budou jeho jménem dodána pouze prostřednictvím zaměstnanců, kteří jsou ve vztahu k charakteru plnění bezúhonní a splňující potřebné kvalifikační předpoklady a že je tuto skutečnost schopen na vyžádání ST/TMCZ prokázat. Tato povinnost platí obdobně pro subdodavatele, kteří se jménem Dodavatele budou podílet na poskytování plnění.*
  8. *Dodavatel bere na vědomí a poučí své Zaměstnance a subdodavatele, že jsou povinni zejména:* 
     1. *pro vstup a výstup do a z prostor ST/TMCZ používat výhradně hlavní vchod; ostatní vchody a východy mohou využít jen ve výjimečných situacích (např.: evakuace, přínos či odnos nadměrného nákladu);*
     2. *tak, kde je vyžadováno, prokázat se bez vyzvání při vstupu do prostor příslušnému zaměstnanci a/nebo pověřené osobě;*
     3. *dbát, aby údaje (pokud jsou požadovány) uvedené na Přístupovém prostředku odpovídaly skutetčnosti;*
     4. *chránit Přístupový prostředek před poškozením, zničením, ztrátou, krádeží a zneužitím jinou osobou;*
     5. *neposkytovat Přístupový prostředek jiným osobám;*
     6. *pokud byl přidělený, tak viditělně nosit průkaz návštěvníka po celou dobu pobytu v prostorách ST/TMCZ;*
     7. *bezodkladně oznámit ST/TMCZ ztrátu, krádež, požkození, zneužití Přístupového prostředku, jakož i jakoukoliv změnu údajů obsaženou na Přístupovém prostředku;*
     8. *na vyzvání zaměstnance ST/TMCZ se prokázat Přístupovým prostředkem;*
     9. *neumožnit vstup do objektu ST/TMCZ žádné osobě;*
     10. *po ukončení smluvní činnosti vrátit Přístupový prostředek, jakož i veškeré další věci náležející ST/TMCZ.*
  9. *Dodavatel a veškeré osoby podílející se na poskytování plnění dle Smlouvy/Objednávky jeho jménem, jsou povinni podřídit se a respektovat zavedené bezpečnostní opatření ST/TMCZ a bezpečnostní pokyny a nejsou oprávněn provádět žádné činnosti, které by mohly tato opatření narušit nebo poškodit.*
  10. *Dodavatel je povinen zajistit ochranu důvěrnosti a integrity Přístupových prostředků (přístupové ID, hesla, tokeny čipové karty, vstupní karty, klíče apod.) do elektronických systémů a prostor ST/TMCZ, které jsou Dodavateli zpřístupněny na základě Smlouvy/Objednávky a/nebo dílčí smlouvy či objednávky a nesmí je zpřístupnit třetím osobám. Dodavatel je povinen neprodleně oznámit ST/TMCZ ztrátu, krádež, zneužití či zničení Přístupového prostředku v souladu bodem č. 20 dokumentu Korporátní pravidla IMS a bezpečnosti a ochrany dat.*
  11. *Dodavatel je vždy povinen informovat ST/TMCZ pokud některá z Pověřených osob ukončí svůj pracovní (dodavatelský) vztah s Dodavatelem a vrátit veškeré poskytnuté Přístupové prostředky, které ST/TMCZ této osobě poskytl. Ztracený Přístupový prostředek je Dodavatel povinen ST/TMCZ nahradit.*
  12. *Důvěrné informace s velkým objemem budou mezi Smluvními stranami předávány a vyměňovány výhradně způsobem, který zaručí důvěrnost a integritu přenášených informací (např.: přenosem pomocí SFTP protokolu soubory, které mají stanovený dohodnutý typ a formát).*
  13. *Smluvní strany zřídí bod kontaktu za účelem řešení veškerých problémů, vzájemné poskytování informací, spolupráce v oblasti bezpečnosti informací a ochrany dat a určí kontaktní osobu. Kontaktní informace této osoby (jméno, příjmení, prac.pozícia, prac. email a prac.tel.číslo) zašlou do 10 dnů od podpisu smlouvy / akceptace objednávky na email: security@t-mobile.cz.V případě změny této osoby je Smluvní strana povinna bezodkladně určit novou kontaktaktní osobu oznámiťt ST/TMCZ její kontaktní informace.*
  14. *Dodavatel je povinen bezodkladně ohlásit ST/TMCZ jakoukoliv nestandardní situaci, podezřelé události, bezpečnostní incidenty a ztrátu Přístupového prostředku a to prostřednictvím následujících konktaktů:*

1. *pro ST: email:* [*security@telekom.sk*](mailto:security@telekom.sk)*, tel .: +421 800 100 166,*
2. *pro TMCZ: email: security@t-mobile.cz, tel .: +421 800 100 166.*

*Dodavatel je povinen v rámci spolupráce s ST/TMCZ vynaložit maximální úsilí, aby zabránil pokračování bezpečnostního incidentu, předešel dalším bezpečnostním incidentům, zajistil a obnovil všechna opatření nezbytná pro ochranu dat a informací ST/TMCZ.*

* 1. *Pokud při plnění Smlouvy/Objednávky dojde k výkonu činností, která přímo souvisí s tím, že (a) Dodavatel zajišťuje funkčnost technických a programových prostředků tvořících informační a/nebo komunikační systém TMCZ a/nebo (b) je takový vztah významný z hlediska bezpečnosti informačního a/nebo komunikačního systému TMCZ a Dodavatel tím naplnil znaky Významného dodavatele definované ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, jsou smluvní strany poviny před započetím těchto činnsoti uzavřít smlouvu o úrovni služeb v oblasti kybernetické bezpečnosti.*
  2. *Za porušení dokumentu Korporátní pravidla IMS a bezpečnosti a ochrany dat má ST/TMCZ právo na smluvní pokutu ve výši 2 500 000 Kč (slovy: dva miliony pět set tisíc). Smluvní pokuta je splatná na základě vystavené faktury ST/TMCZ bez zbytečného odkladu po porušení smluvních povinností, a to do 14 dnů od jejího vystavení. Dodavatel se zavazuje, že smluvní pokutu zaplatí řádně a včas. Uhrazením smluvní pokuty nezaniká právo ST/TMCZ na náhradu škody v plném rozsahu.*
  3. *Dodavatel je povinen zajistit, aby jím Pověřené osoby dodržovaly platná režimová, technická a organizační opatření upravující řízení vstupu, pohybu osob a dopravních prostředků v prostorách a objektech ST/TMCZ. Pro umožnění vstupu osob a/nebo vjezd dopravních prostředků do prostor a objektů ST/TMCZ bude Dodavateli vydáno potřebné povolení vydané příslušným oddělení ST/TMCZ. Dodavatel si o povolení požádá prostřednictvím konktaktní osoby dle bodu čl.19 dokumentu Korporátní pravidla IMS a bezpečnosti a ochrany dat..*
  4. *Za seznámení Pověřených osob Dodavatele s relevantními interními předpisy ST/TMCZ, odevzdání Přístupových prostředků určených pro Pověřené osoby odpovídá odpovědná osoba ST/TMCZ.*
  5. *Dodavatel bere na vědomí, že jím Pověřené osoby se podrobí kontrole vykonávané v souladu s interními předpisy ST/TMCZ (např.: fyzická kontrola osob a dopravních prostředků, technická kontrola zařízení) při vstupu do prostor ST/TMCZ. Pověřené osoby, které vykonávají činnost v prostorách ST/TMCZ jsou poviny se před vstupem do těchto prostor identifikovat (např.: zaměstnaneckým průkazem, průkazem totožnosti, občanským průkazem, cestovním pasem).*
  6. *V případě, že Dodavateli budou odevzdány Přístupové prostředky do prostor či objektů ST/TMCZ, je Dodavatel povinen dodržovat interní předpisy ST/TMCZ týkající se Přístupových prostředků. Dodavatel nesmí vyhotovit duplikát či kopii z převzatého Přístupového prostředku.*
  7. *Dodavatel a jím Pověřené osoby jsou oprávněny při výkonu plnění dle této Smlouvy/Objednávky zdržovat se a pohybovat se v prostorách a objektech ST/TMCZ jen v čase potřebném pro uskutečnění smluvně dohodnutých činností a služeb a jen v prostorách a objektech, které jsou pro tyto činnosti určeny.*
  8. *Dodavatel je povinen zabezpečit, aby zdrojový kód, který dodá v rámci spolupráce, obsahoval jen kód vyvinutý v souladu s požadavky Smlouvy/Objednávky, bezpečnostní dokumentaci ST/TMCZ a v souladu s aplikovatelnými standardy dle bodu 1. Dodavatel se zejména zavazuje, že zdrojový kód nebude obsahovat žádné zlomyslné a/nebo škodlivé prvky či bezpečnostní slabiny umožňující narušení bezpečnosti předmětu Smlouvy/Objednávky, a že nebude obsahovat žádný Mallware. Přístup ke zdrojovému kódu bude Dodavatel řídit, omezovat na nevyhnutelný okruh Pověřených osob a chránit proti neoprávněné manipulaci.*
  9. *Mallwarem se rozumí zejména jakýkoliv počítačový program, soubor příkazů a instrukcí použitých přímo nebo nepřímo v počítači se schopností poškodit, zasahovat, narušit a/nebo jakkoliv nepříznivě ovlivnit softwary, počítačové programy, datové soubory a/nebo činnost jakéhokoliv hadwaru, mobilních a jiných koncových zařízení a/nebo síťových funkcionalit včetně virů, červů (worms), trojských koní (trojan horse), spyware, zadních vrátek (back doors) a jiných programů, které úmyslně uskutečňují jakékoliv zbytečné, narušující a/nebo ničivé funkce v rámci informačního systému.*
  10. *Dodavatel je povinen zabezpečit:*
      + - 1. *že pro vývojové a testovací účely použije samostatně vyvinuté testovací anonymizovaná data,*
          2. *ochranu důvěrnosti, dostupnosti a integrity testovacích dat,*
          3. *samostatné vývojové a testovací prostředí oddělené od živého provozního systému,*
          4. *bezodkladnou bezpečnou prokazatelnou likvidaci testovacích dat po skončení potřeby jejich použití,*
          5. *před odevzdáním plnění dle této Smlouvy/Objednávky do provozu akceptační testy, jejichž součástí jsou i bezpečnostní testy.*

**Příloha č. 1 – Příloha o bezpečnosti informací**



**Příloha č. 2 – BCM Požadavky**



**Příloha č. 3 – Schválení subdodavatelé**

